



# UNITED STATES PATENT AND TRADEMARK OFFICE.

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/886,515	06/21/2001	Francisco J. Villavicencio	21756-011800	5483
51206	7590	09/07/2006	EXAMINER	
TOWNSEND AND TOWNSEND AND CREW LLP TWO EMBARCADERO CENTER 8TH FLOOR SAN FRANCISCO, CA 94111-3834			BAUM, RONALD	
			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 09/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/886,515

Applicant(s)

VILLAVICENCIO ET AL

Examiner

Ronald Baum

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 6/13/2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-60, 62, 63 and 65 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-25, 32-37, 42-45 and 50-54 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 20060830.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

**DETAILED ACTION**

1. This action is in reply to applicant's correspondence of 13 June 2006.
2. Claims 1-65 are pending for examination.
3. Claims 1-25,32-37,42-45,50-54 remain rejected.

***Claim Rejections - 35 USC § 102***

The examiner acknowledges and thanks the applicant for pointing out the typographical error concerning the 35 U.S.C. 102 paragraph rejection in the previous office action.

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-25,32-37,42-45,50-54 are rejected under 35 U.S.C. 102(e) as being anticipated by Olden, U.S. Patent 6,460,141 B1.

5. As per claim 1; "A method for providing access to resources [Abstract, figures 1-33 and accompanying descriptions], comprising the steps of:

acquiring user identification information from a first authentication system,

said user identification information is associated with a request from a first user to access a first resource,

said step of acquiring is performed by an authorization system,

said authorization system is separate from said first authentication system [figures 1-5 and accompanying descriptions, whereas the authorization component, entitlement server component, administrative client/resource consumer (at the user, group, and realm level insofar as user identification information would be concerned), and enabled web server, as broadly interpreted by the examiner correspond respectively, to the applicant's authorization system, first authentication system, user identification information (source thereof), and accessible resources.];

relying on said first authentication system for authenticating said first user;

using said user identification information to access an identity profile associated with said user identification information [figures 1-5, and particularly figures 2,3, and accompanying descriptions, whereas the entitlement creation/assignment in the access rights, user/group/realm information (i.e., the database referencing aspects thereof) pertaining to user ID, name, address, password, ACL analog, etc., aspects, as broadly interpreted by the examiner correspond, to the applicant's '... using said user ... information to access ... profile ...'.]; and

performing, at said authorization system, authorization services for said request to access said first resource based on said identity profile associated with said user identification information [figures 1-33, and accompanying descriptions, whereas the actual authorization servicing functionality per se, as broadly interpreted by the examiner correspond, to the applicant's '... performing authorization services ...'.];

wherein said authorization services comprise determining whether said first user is authorized to access said first resource [figures 1-33, and accompanying descriptions, whereas

Art Unit: 2136

the actual authorization servicing functionality per se, as broadly interpreted by the examiner correspond, to the applicant's claim limitation.]; and

wherein authenticating said first user comprises verifying an identity of said first user [figures 1-5, and particularly figures 2,3, and accompanying descriptions, whereas the entitlement creation/assignment in the access rights, user/group/realm information (i.e., the database referencing aspects thereof) pertaining to user ID, name, address, password, ACL analog, etc., aspects, as broadly interpreted by the examiner correspond, to the applicant's claim limitation.].”;

Further, as per claim 32, this claim is the embodied method software for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection;

6. Claim 2 ***additionally recites*** the limitation that; “A method according to claim 1, wherein: said step of acquiring user identification includes reading a user ID from an internal web server variable.”.

The teachings of Olden are directed towards such limitations (i.e., col. 23, lines 45-col. 24, line 57, whereas the ‘... cookie is created for each user ...’ which clearly is a web server variable (i.e., cookie) based on user information/ID/variables and the transfer thereof, as broadly interpreted by the examiner would clearly encompass ‘... acquiring user identification ... user ID ... web server variable ...’).

7. Claim 3 *additionally recites* the limitation that; “A method according to claim 2, further comprising the step of:

allowing a first user to access said first resource if said step of performing determines that said first user is authorized to access said first resource based on said identity profile, said first user is associated with said identity profile and said request.”.

The teachings of Olden are directed towards such limitations (i.e., figures 1-33, and accompanying descriptions, whereas the actual authorization servicing functionality and subsequent resource access (i.e., retrieve a web document/file/page) per se, as broadly interpreted by the examiner correspond, to the applicant's ‘... access ... resource ... authorized to access ... resource ... profile...’).

8. Claim 4 *additionally recites* the limitation that; “A method according to claim 1, wherein relying on said first authentication system comprises the steps of:

receiving information about said request;

determining whether said first resource is protected; and

determining that authentication for said first resource is to be performed by said first authentication system.”.

The teachings of Olden are directed towards such limitations (i.e., figures 1-33, and particularly figure 28, and accompanying descriptions, whereas the actual authorization servicing functionality and subsequent resource access (i.e., retrieve a web document/file/page) per se, inherently require the setup of access requirements in order to create the user/group/realm levels of access criteria as related to the associated resources in question (i.e., to protect or not, and at

what level of secured protection), as broadly interpreted by the examiner correspond, to the applicant's '... determining ... resource is protected; ... authentication ... resource is to be performed ...').

Further, as per the claim 33 *additionally recited* limitation, this claim is the embodied method software for the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection.

9. Claim 5 *additionally recites* the limitation that; "A method according to claim 1, wherein: said step of acquiring user identification includes acquiring a plurality of data items which can be used to identify a user."

The teachings of Olden are directed towards such limitations (i.e., col. 7, lines 10-col. 8, line 5, whereas the actual authorization servicing functionality and subsequent resource access (i.e., retrieve a web document/file/page) per se, inherently require the setup of access requirements in order to create the user/group/realm levels of access criteria as related to the associated resources in question (i.e., to protect or not, and at what level of secured protection), and further, such user level criteria such as "for example, user ID, first name, last name ...", as broadly interpreted by the examiner correspond, to the applicant's '... acquiring user identification ... plurality of data items ... identify a user ...').

10. Claim 6 *additionally recites* the limitation that; "A method according to claim 1, further comprising the step of:

acquiring one or more data items in addition to said user identification information, said step of performing authorization services uses said one or more data items to attempt to authorize access to said first resource in response to said request.”.

The teachings of Olden are directed towards such limitations (i.e., col. 7, lines 10-col. 8, line 5, whereas the actual authorization servicing functionality and subsequent resource access (i.e., retrieve a web document/file/page) per se, inherently require the setup of access requirements (i.e., one or more data items) in order to create the user/group/realm levels of access criteria as related to the associated resources in question (i.e., to protect or not, and at what level of secured protection), and further, such user level criteria such as “for example, user ID, first name, last name ... as well as *extendible attributes* ...”, as broadly interpreted by the examiner correspond, to the applicant’s ‘ ... acquiring ... data items in addition ... identification information, ... authorization services uses said one or more data ...’.).

Further, as per the claim 34 *additionally recited* limitation, this claim is the embodied method software for the method claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection.

11. Claim 7 *additionally recites* the limitation that; “A method according to claim 1, wherein: said authorization system is part of an access system that protects a plurality of resources, said plurality of resources includes said first resource, a second resource and a third resource;  
said first resource uses said first authentication system for authentication services;



said second resource uses a second authentication system for authentication services,  
said second authentication system is separate from said access system; and  
said third resource uses a third authentication system for authentication services,  
said third authentication system is separate from said access system.”.

The teachings of Olden are directed towards such limitations (i.e., col. 3, lines 24-col. 4, line 45, col. 6, lines 36-62, col. 9, lines 63-col. 11, line 54, col. 19, lines 43-col. 20, line 57, whereas the ‘... plurality of authorization servers ... at least one authorization dispatcher ... communicate with the entitlements server component ...’ which clearly encompasses plural authentication/authorization/access to resources aspects, as broadly interpreted by the examiner would clearly encompass ‘... authorization system is part ... protects a plurality of resources, ... said first resource uses said first authentication system for authentication services; said second resource ... said third resource ... authentication system ...’).

12. Claim 8 *additionally recites* the limitation that; “A method according to claim 7, wherein:  
said first authentication system is a default web server authentication system;  
said second authentication system is an authentication plug-in; and  
said third authentication system is a third party authentication system.”.

The teachings of Olden are directed towards such limitations (i.e., col. 3, lines 24-col. 4, line 45, col. 6, lines 36-62, col. 9, lines 63-col. 11, line 54, col. 19, lines 43-col. 20, line 57, whereas the ‘... plurality of authorization servers ... at least one authorization dispatcher ... communicate with the entitlements server component ... Web server plug-ins are started... cookies ... Web server plug-ins ...’ which clearly encompasses plural authentication/authorization/access to resources

aspects, as broadly interpreted by the examiner would clearly encompass ‘ ... first authentication system ... default web server ... second authentication ... plug-in; and said third authentication ... third party authentication system...’).

13. Claim 9 ***additionally recites*** the limitation that; “A method according to claim 1, wherein: said authorization system is part of an access system that protects a plurality of resources, said access system provides for use of one or more internal authentication systems and said access system provides for reliance on one or more external authentication systems, said one or more external authentication systems include said first authentication system.”.

The teachings of Olden are directed towards such limitations (i.e., col. 3, lines 24-col. 4, line 45, col. 6, lines 36-62, col. 9, lines 63-col. 11, line 54, col. 19, lines 43-col. 20, line 57, whereas the ‘... plurality of authorization servers ... at least one authorization dispatcher ... communicate with the entitlements server component ...’ which clearly encompasses plural authentication/authorization/access to resources aspects, insofar as the inherent robust nature of the network architecture, inclusive of the *intranet* (i.e., internal server aspects) and *Internet web* (i.e., external server aspects) as broadly interpreted by the examiner would clearly encompass ‘ ... authorization system ... access system that protects a plurality of resources, ... internal authentication systems ... reliance ... external authentication systems, ... first authentication system ...’).

Further, as per the claim 35 *additionally recited* limitation, this claim is the embodied method software for the method claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection.

14. Claim 10 *additionally recites* the limitation that; "A method according to claim 1, wherein:

said authorization system is part of an access system that protects a plurality of resources and

does not have an applications program interface."

The teachings of Olden are directed towards such limitations (i.e., col. 3, lines 24-col. 4, line 45, col. 6, lines 36-62, col. 9, lines 63-col. 11, line 54, col. 19, lines 43-col. 20, line 57, whereas the '... plurality of authorization servers ... at least one authorization dispatcher ... communicate with the entitlements server component ...' which clearly encompasses plural authentication/authorization/access to resources aspects, insofar as the inherent robust nature of the network architecture, inclusive of the *intranet* (i.e., internal server aspects) and *Internet web* (i.e., external server aspects) as broadly interpreted by the examiner would clearly encompass '... authorization system ... access system that protects a plurality of resources, ... does not have an applications program interface ...').

15. Claim 11 *additionally recites* the limitation that; "A method according to claim 1, further comprising the steps of:

using said user identification information to create information for a cookie; and

causing said cookie to be transmitted for storage on a client associated with said request.”.

The teachings of Olden are directed towards such limitations (i.e., col. 23, lines 45-col. 24, line 57, whereas the ‘... cookie is created for each user ...’ which clearly is a cookie based on user information/variables and the transfer thereof, as broadly interpreted by the examiner would clearly encompass ‘... using ... information to create ... cookie; ... storage on a client ...’).

16. Claim 12 *additionally recites* the limitation that; “A method according to claim 11, further comprising the step of:

performing single sign-on services based on said cookie.”.

The teachings of Olden are directed towards such limitations (i.e., col. 23, lines 45-col. 24, line 57, whereas the ‘... supports single sign on ... cookie is created for each user ... eliminating the need ... submit ... *password again*’ which clearly is a cookie based on user information/variables and the transfer thereof, as broadly interpreted by the examiner would clearly encompass ‘... single sign-on services based on said cookie ...’).

Further, as per the claim 36 *additionally recited* limitation, this claim is the embodied method software for the method claims 11,12 above, and is rejected for the same reasons provided for the claims 11,12 rejection.

17. Claim 13 *additionally recites* the limitation that; “A method according to claim 11, further comprising the steps of:

receiving a request to access a second resource,

said request to access said second resource includes contents of said cookie; and

using said cookie to authorize access to said second resource without authenticating.”.

The teachings of Olden are directed towards such limitations (i.e., col. 23, lines 45-col. 24, line

57, whereas the ‘... supports single sign on ... cookie is created for each user ... eliminating the need ... submit ... *password again*’ which clearly is a cookie based on user

information/variables and the transfer thereof, as broadly interpreted by the examiner would

clearly encompass ‘... using ... information to create ... cookie; ... storage on a client ... cookie to authorize access ... without authenticating’.).

18. Claim 14 *additionally recites* the limitation that; “A method according to claim 11, further comprising the steps of:

receiving a request to access a second resource at a second server,

said request to access said first resource was received at a first server but not at said second server,

said first authentication system does include said first server and does not include said second server,

said step of receiving said request to access said second resource includes receiving contents of said cookie; and

using said cookie at said second server to authorize access to said second resource without authenticating.”.

The teachings of Olden are directed towards such limitations (i.e., col. 23, lines 45-col. 24, line 57, whereas the ‘... supports single sign on ... cookie is created for each user ... eliminating the need ... submit ... *password again*’ which clearly is a cookie based on user information/variables and the transfer thereof, and further, the inherent nature of cookie creation/transfer is such that the cookies have a basically one-to-one relationship between the server and client so associated. Still further, the IP routing nature of the Internet embodied (at the least) embodiment would route packets such that rejection of non-addressed packets would inherently occur, such that, as broadly interpreted by the examiner would clearly encompass ‘... using ... information to create ... cookie; ... storage on a client ... cookie to authorize access ... (multiple server resources) ... without authenticating’.).

Further, as per the claim 37 *additionally recited* limitation, this claim is the embodied method software for the method claims 11,14 above, and is rejected for the same reasons provided for the claims 11,14 rejection.

19. As per claim 15; “A method for providing access to resources [Abstract, figures 1-33 and accompanying descriptions], comprising the steps of:

- acquiring a plurality of variables from a first authentication system,
- said step of acquiring is performed by an authorization system,
- said authorization system is separate from said first authentication system,
- said variables are associated with a first request from a first user to access a first resource [figures 1-5 and accompanying descriptions, whereas the authorization

component, entitlement server component, administrative client/resource consumer (at the user, group, and realm level insofar as user identification information/ plurality of variables would be concerned), and enabled web server, as broadly interpreted by the examiner correspond respectively, to the applicant's authorization system, first authentication system, user identification information/ plurality of variables (source thereof), and accessible resources.];

relying on said first authentication system for authenticating said first user; performing, at said authorization system, authorization services for said request to access said first resource based on said plurality of variables [figures 1-33, and accompanying descriptions, whereas the actual authorization servicing functionality per se, as broadly interpreted by the examiner correspond, to the applicant's ' ... performing authorization services ... '];

wherein said authorization services comprise determining whether said first user is authorized to access said first resource [figures 1-33, and accompanying descriptions, whereas the actual authorization servicing functionality per se, as broadly interpreted by the examiner correspond, to the applicant's claim limitation.]; and

wherein authenticating said first user comprises verifying an identity of said first user [figures 1-5, and particularly figures 2,3, and accompanying descriptions, whereas the entitlement creation/assignment in the access rights, user/group/realm information (i.e., the database referencing aspects thereof) pertaining to user ID, name, address, password, ACL analog, etc., aspects, as broadly interpreted by the examiner correspond, to the applicant's claim limitation.]”.

Further, as per claim 42, this claim is the embodied method software for the method claim 15 above, and is rejected for the same reasons provided for the claim 15 rejection.

20. Claim 16 *additionally recites* the limitation that; “A method according to claim 15, wherein relying on said first authentication system comprises the steps of:

receiving information from said first request;

determining whether said first resource is protected; and

determining that authentication for said first resource is to be performed by said first authentication system.”.

The teachings of Olden are directed towards such limitations (i.e., figures 1-33, and particularly figure 28, and accompanying descriptions, whereas the actual authorization servicing functionality and subsequent resource access (i.e., retrieve a web document/file/page) per se, inherently require the setup of access requirements in order to create the user/group/realm levels of access criteria as related to the associated resources in question (i.e., to protect or not, and at what level of secured protection), as broadly interpreted by the examiner correspond, to the applicant’s ‘... determining ... resource is protected; ... authentication ... resource is to be performed ...’).

Further, as per the claim 43 *additionally recited* limitation, this claim is the embodied method software for the method claim 16 above, and is rejected for the same reasons provided for the claim 16 rejection.



21. Claim 17 *additionally recites* the limitation that; “A method according to claim 15, wherein:

said authorization system is part of an access system that protects a plurality of resources,  
said access system provides for use of one or more internal authentication systems and  
said access system provides for reliance on one or more external authentication systems,  
said one or more external authentication systems include said first authentication system.”.

The teachings of Olden are directed towards such limitations (i.e., col. 3, lines 24-col. 4, line 45, col. 6, lines 36-62, col. 9, lines 63-col. 11, line 54, col. 19, lines 43-col. 20, line 57, whereas the ‘... plurality of authorization servers ... at least one authorization dispatcher ... communicate with the entitlements server component ...’ which clearly encompasses plural authentication/authorization/access to resources aspects, insofar as the inherent robust nature of the network architecture, inclusive of the *intranet* (i.e., internal server aspects) and *Internet web* (i.e., external server aspects) as broadly interpreted by the examiner would clearly encompass ‘... authorization system ... access system that protects a plurality of resources, ... internal authentication systems ... reliance ... external authentication systems, ... first authentication system ...’.).

Further, as per the claim 44 *additionally recited* limitation, this claim is the embodied method software for the method claim 17 above, and is rejected for the same reasons provided for the claim 17 rejection.

22. Claim 18 *additionally recites* the limitation that; “A method according to claim 15, further comprising the steps of:

using said plurality of variables to create information for a cookie; and

causing said cookie to be transmitted for storage on a client associated with said

request.”.

The teachings of Olden are directed towards such limitations (i.e., col. 23, lines 45-col. 24, line 57, whereas the ‘... cookie is created for each user ...’ which clearly is a cookie based on user information/variables and the transfer thereof, as broadly interpreted by the examiner would clearly encompass ‘... using ... plurality of variables to create ... cookie; ... storage on a client ...’).

23. Claim 19 *additionally recites* the limitation that; “A method according to claim 18, further comprising the step of:

performing single sign-on services based on said cookie.”.

The teachings of Olden are directed towards such limitations (i.e., col. 23, lines 45-col. 24, line 57, whereas the ‘... supports single sign on ... cookie is created for each user ...’ which clearly is a cookie based on user information/variables and the transfer thereof, as broadly interpreted by the examiner would clearly encompass ‘... single sign-on services based on said cookie ...’).

24. Claim 20 *additionally recites* the limitation that; “A method according to claim 18, further comprising the steps of:

receiving a request to access a second resource at a second server,

said request to access said first resource was received at a first server but not at said second server,

said first authentication system does include said first server and does not include said second server,

said step of receiving said request to access said second resource includes receiving contents of said cookie; and using said cookie at said second server to authorize access to said second resource without authenticating.”.

The teachings of Olden are directed towards such limitations (i.e., col. 23, lines 45-col. 24, line 57, whereas the ‘... supports single sign on ... cookie is created for each user ... eliminating the need ... submit ... *password again*’ which clearly is a cookie based on user information/variables and the transfer thereof, and further, the inherent nature of cookie creation/transfer is such that the cookies have a basically one-to-one relationship between the server and client so associated. Still further, the IP routing nature of the Internet embodied (at the least) embodiment would route packets such that rejection of non-addressed packets would inherently occur, such that, as broadly interpreted by the examiner would clearly encompass ‘... using ... information to create ... cookie; ... storage on a client ... cookie to authorize access ... (multiple server resources) ... without authenticating’.).

Further, as per the claim 45 *additionally recited* limitation, this claim is the embodied method software for the method claims 18,20 above, and is rejected for the same reasons provided for the claims 18,20 rejection.

25. As per claim 21; “A method for providing access to resources [Abstract, figures 1-33 and accompanying descriptions], comprising the steps of:

acquiring user identification information from an authentication system,

said user identification information is associated with a request from a first user to access a first resource,

said step of acquiring is performed by an authorization system,

said authorization system is separate from said authentication system

[figures 1-5 and accompanying descriptions, whereas the authorization

component, entitlement server component, administrative client/resource

consumer (at the user, group, and realm level insofar as user identification

information would be concerned), and enabled web server, as broadly interpreted

by the examiner correspond respectively, to the applicant's authorization system,

first authentication system, user identification information (source thereof), and

accessible resources.];

relying on said authentication system for authenticating said first user;

using said user identification information to create information for a cookie;

causing said cookie to be transmitted for storage on a client associated with said request

to access said first resource [i.e., col. 23, lines 45-col. 24, line 57, whereas the ‘... cookie is

created for each user ...' which clearly is a cookie based on user information/variables and the transfer thereof, as broadly interpreted by the examiner would clearly encompass ' ... using ... information to create ... cookie; ... storage on a client ...'.]; and

performing, at said authorization system, authorization services for said request to access said first resource [figures 1-33, and accompanying descriptions, whereas the actual authorization servicing functionality per se, as broadly interpreted by the examiner correspond, to the applicant's ' ... performing authorization services ...'.];

wherein said authorization services comprise determining whether said first user is authorized to access said first resource [figures 1-33, and accompanying descriptions, whereas the actual authorization servicing functionality per se, as broadly interpreted by the examiner correspond, to the applicant's claim limitation.]; and

wherein authenticating said first user comprises verifying an identity of said first user [figures 1-5, and particularly figures 2,3, and accompanying descriptions, whereas the entitlement creation/assignment in the access rights, user/group/realm information (i.e., the database referencing aspects thereof) pertaining to user ID, name, address, password, ACL analog, etc., aspects, as broadly interpreted by the examiner correspond, to the applicant's claim limitation.]"

Further, as per claim 50, this claim is the embodied method software for the method claim 21 above, and is rejected for the same reasons provided for the claim 21 rejection.

Art Unit: 2136

26. Claim 22 *additionally recites* the limitation that, "A method according to claim 21, wherein:

said authorization system is part of an access system that protects a plurality of resources,

said access system provides for use of one or more internal authentication systems

and

said access system provides for reliance on one or more external authentication

systems,

said one or more external authentication systems include said first

authentication system."

The teachings of Olden are directed towards such limitations (i.e., col. 3, lines 24-col. 4, line 45, col. 6, lines 36-62, col. 9, lines 63-col. 11, line 54, col. 19, lines 43-col. 20, line 57, whereas the '... plurality of authorization servers ... at least one authorization dispatcher ... communicate with the entitlements server component ...' which clearly encompasses plural authentication/authorization/access to resources aspects, insofar as the inherent robust nature of the network architecture, inclusive of the *intranet* (i.e., internal server aspects) and *Internet web* (i.e., external server aspects) as broadly interpreted by the examiner would clearly encompass '... authorization system ... access system that protects a plurality of resources, ... internal authentication systems ... reliance ... external authentication systems, ... first authentication system ...').

Further, as per the claim 51 *additionally recited* limitation, this claim is the embodied method software for the method claim 22 above, and is rejected for the same reasons provided for the claim 22 rejection.

27. Claim 23 *additionally recites* the limitation that; “A method according to claim 21, further comprising the step of:

performing single sign-on services based on said cookie.”.

The teachings of Olden are directed towards such limitations (i.e., col. 23, lines 45-col. 24, line 57, whereas the ‘... supports single sign on ... cookie is created for each user ... eliminating the need ... submit ... *password again*’ which clearly is a cookie based on user information/variables and the transfer thereof, as broadly interpreted by the examiner would clearly encompass ‘... single sign-on services based on said cookie ...’).

Further, as per the claim 52 *additionally recited* limitation, this claim is the embodied method software for the method claim 23 above, and is rejected for the same reasons provided for the claim 23 rejection.

28. Claim 24 *additionally recites* the limitation that; “A method according to claim 21, further comprising the steps of:

receiving a request to access a second resource,

said request to access said second resource includes contents of said cookie; and

using said cookie to authorize access to said second resource without authenticating.”.

The teachings of Olden are directed towards such limitations (i.e., col. 23, lines 45-col. 24, line 57, whereas the ‘... supports single sign on ... cookie is created for each user ... eliminating the need ... submit ... *password again*’ which clearly is a cookie based on user information/variables and the transfer thereof, as broadly interpreted by the examiner would clearly encompass ‘... using ... information to create ... cookie; ... storage on a client ... cookie to authorize access ... without authenticating’.).

Further, as per the claim 53 ***additionally recited*** limitation, this claim is the embodied method software for the method claim 24 above, and is rejected for the same reasons provided for the claim 24 rejection.

29. Claim 25 ***additionally recites*** the limitation that; “A method according to claim 21, further comprising the steps of:

receiving a request to access a second resource at a second server,

said request to access said first resource was received at a first server but not at said second server,

said first authentication system does include said first server and does not include said second server,

said step of receiving said request to access said second resource includes receiving contents of said cookie; and

using said cookie at said second server to authorize access to said second resource without authenticating.”.



The teachings of Olden are directed towards such limitations (i.e., col. 23, lines 45-col. 24, line 57, whereas the ‘... supports single sign on ... cookie is created for each user ... eliminating the need ... submit ... *password again*’ which clearly is a cookie based on user information/variables and the transfer thereof, and further, the inherent nature of cookie creation/transfer is such that the cookies have a basically one-to-one relationship between the server and client so associated. Still further, the IP routing nature of the Internet embodied (at the least) embodiment would route packets such that rejection of non-addressed packets would inherently occur, such that, as broadly interpreted by the examiner would clearly encompass ‘... using ... information to create ... cookie; ... storage on a client ... cookie to authorize access ... (multiple server resources) ... without authenticating’.).

Further, as per the claim 54 *additionally recited* limitation, this claim is the embodied method software for the method claim 25 above, and is rejected for the same reasons provided for the claim 25 rejection.

#### ***Allowable Subject Matter***

30. Claims 26-31, 38-41, 46-49, 55-60, 62, 63, 65 allowed over prior art.

#### ***Response to Amendment***

31. As per applicant’s argument concerning the lack of teaching by Olden of a “separate” network system configuration aspects, the examiner has fully considered in this response to

Art Unit: 2136

amendment; the arguments, and finds them still not to be persuasive, as per the previous office action arguments response.

32. As per applicant's argument concerning the lack of teaching by Olden of an "external " network system configuration aspects, the examiner has fully considered in this response to amendment; the arguments, and finds them to be persuasive. The claims 26-31,38-41,46-49,55-60,62,63,65, whereas the reference is to "external" network system configuration are allowed over prior art.

***Conclusion***

33. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

NASSER MOAZZAM  
PRIMARY EXAMINER

  
9/11/06

